

12 FAM 260

COUNTERINTELLIGENCE

(TL:DS-72; 01-26-2001)

12 FAM 261 GENERAL

12 FAM 261.1 Program Implementation

(TL:DS-72; 01-26-2001)

a. The Department's counterintelligence program is defensive in nature. Its purpose is to deter, detect, and neutralize the threat posed by hostile intelligence services against U.S. diplomatic personnel, facilities, equipment, and information. This protection extends to the Department's direct-hire employees as well as to contractors and dependents of U.S. Government personnel serving abroad under the authority of a chief of mission.

b. The Office of Investigations and Counterintelligence (DS/DSS/ICI) is responsible for the implementation of all counterintelligence programs, which DS coordinates with INR and other members of the U.S. intelligence community. DS/DSS/ICI conducts counterintelligence investigations (see 1 FAM 262.4) and implements the programs described in this subchapter.

12 FAM 261.2 Authority

(TL:DS-62; 11-22-1999)

(Effective Date: 02-08-1999)

a. The Omnibus Diplomatic Security and Antiterrorism Act of 1986, Section 103, authorizes the Secretary of State to develop and implement policies and programs which provide for the security of U.S. Government operations of a diplomatic nature, and foreign government operations of a diplomatic nature in the United States. This mission includes consultation with Federal agencies having personnel under the authority of a chief of mission.

b. The Secretary of State is authorized to develop and implement a special personnel security program for Department employees who are responsible for security at diplomatic and consular posts in high intelligence threat countries in accordance with Pub. L. 100-204, Section 155(a).

c. E.O. 10450 requires the investigation of civilian officers and employees to ensure that their initial and continued employment is clearly consistent with national security.

d. 5 U.S.C. 301 authorizes heads of agencies to prescribe regulations regarding the conduct of employees.

e. 22 U.S.C. 842 gives the Secretary of State authority to prescribe regulations relating to duties, functions, and obligations of Department employees (see 3 FAM).

12 FAM 261.3 Counterintelligence Working Groups

(TL:DS-62; 11-22-1999)

(Effective Date: 02-08-1999)

a. Counterintelligence working groups (CIWGs) review post-specific counterintelligence issues on a periodic basis and are chaired by the deputy chief of mission. DS/ICI/CAS provides guidance and advice, as necessary, to post CIWGs that perform the following functions:

- (1) Evaluate human intelligence and technical threats posed by host government and/or foreign intelligence services;
- (2) Determine the level of vulnerability of existing personnel and facilities;
- (3) Take appropriate actions to counter an identified threat;
- (4) Monitor the effectiveness of existing counterintelligence plans, programs, and practices; and
- (5) Coordinate all post counterintelligence programs.

b. See 12 FAH-6, *OSPB Security Standards and Policy Handbook*, for CIWG reporting requirements and meeting frequencies. A report of issues addressed at each meeting is submitted to DS/ICI/CAS.

12 FAM 261.4 Counterintelligence Surveys

(TL:DS-39; 08-15-1994)

a. DS/ICI/CAS performs counterintelligence surveys at posts identified by the DS Composite Threat List as having a critical or high human intelligence threat. Although surveys are intended for only critical and high human intelligence threat posts, any RSO may request that DS/ICI/CAS perform a counterintelligence survey based on a changing threat environment.

b. Counterintelligence surveys provide:

- (1) An analysis of the human intelligence threat at post;

(2) An evaluation of the effectiveness of existing post countermeasures; and

(3) Recommendations for improving those countermeasures.

12 FAM 262 SECURITY AWARENESS AND CONTACT REPORTING

12 FAM 262.1 Policy

(TL:DS-72; 01-26-2001)

a. The President has directed that each Department or agency of the U.S. Government shall establish procedures, in consultation with the Department of Justice, which require its employees to report all contacts with individuals of any nationality, either within or outside the scope of the employee's official activities, whenever:

(1) Illegal or unauthorized access is sought to classified or otherwise sensitive information; or

(2) The employee is concerned that he or she may be the target of actual or attempted exploitation by a foreign entity.

b. Employees must also report the initial contact with a national from a country with critical threat (counterintelligence) posts listed on the Department's Security Environment Threat List when that national attempts to establish recurring contact or seems to be actively seeking a close personal association, beyond professional or personal courtesies.

c. The purpose of this policy is to protect the security of the United States and its employees, while ensuring the privacy of employees and their freedom of association. This policy seeks to ensure that security risks to persons or to the U.S. Government are identified at the earliest possible opportunity and deterred, and that protective steps are taken to avoid compromise of U.S. employees and national security interests.

d. Reporting contacts under this policy is not accomplished by, nor does it constitute reporting required by 3 FAM 4180 - *Marriage, Equivalent Bonds and Cohabitation*.

12 FAM 262.1-1 Application

(TL:DS-62; 11-22-1999)

(Effective Date: 02-08-1999)

a. These regulations apply abroad to all U.S. citizen employees of the U.S. Government, civilian or military, including contract employees, whether permanently assigned or TDY, who are under the authority of a

chief of mission. Domestically, these regulations apply to employees and contractors of the Department of State. These regulations do not apply domestically to employees of U.S. Government agencies other than the Department of State.

b. Employees with Special Access clearances must follow additional security requirements, as mandated by specific programs, including those of the Director of Central Intelligence (See DCID—Nos. 1/14 and 1/19).

12 FAM 262.1-2 Legal Authorities

(TL:DS-62; 11-22-1999)
(Effective Date: 02-08-1999)

a. Title I of Pub. L. 99-399, the Omnibus Diplomatic Security and Antiterrorism Act of 1986, as amended, codified at 22 U.S.C., Section 4801 et seq.

b. Presidential Decision Directive of August 5, 1993 entitled, "Security Awareness and Reporting of Foreign Contacts" (PDD/NSC-12).

12 FAM 262.1-3 Implementation

(TL:DS-72; 01-26-2001)

The Division of Counterintelligence (DS/ICI/CI) is responsible for administering this program domestically for the Department and abroad through regional security officers.

12 FAM 262.2 Security Awareness and Counseling

(TL:DS-72; 01-26-2001)

a. The regional security officer (RSO) or the post security officer (PSO) shall give an arrival briefing to all employees and contractors assigned to post on permanent change of station. The briefing shall include information on counterintelligence issues of concern at post. TDY personnel shall be briefed on contact reporting responsibilities and other counterintelligence issues, as appropriate, but in every case if the TDY is over 25 days. The RSO or PSO is also available to brief adult dependents of employees and contractors on a voluntary basis. (See 12 FAM 263 - *Counterintelligence Awareness Program*.) *Domestically, employees will be briefed on counterintelligence issues through their bureau unit security officer (USO).*

b. *When an employee reports a contact, the RSO abroad and DS/ICI/CI domestically will conduct checks to determine if information is available indicating that the foreign national has a background connected with intelligence gathering. The RSO or DS/ICI/CI will then discuss the results of the checks with the employee.*

c. The success of this policy is dependent upon the security awareness of *each* employee and upon *each employee's* understanding of and cooperation with its intent. Employees should be alert to any suspicious activity or approach by individuals of any nationality. At post, if an employee is unsure about the circumstances of a contact, *the employee* should discuss the situation with the RSO or PSO, to determine whether filing a report is necessary. In the United States, employees should consult with *DS/ICI/CI*.

12 FAM 262.3 Responsibilities and Procedures

12 FAM 262.3-1 Regional and Post Security Officers

(TL:DS-62; 11-22-1999)
(Effective Date: 02-08-1999)

a. The RSO or PSO will brief all mission employees, TDY employees and contractors about the contact reporting policy and obtain their signatures on an Acknowledgement of Policy Format, such as shown at 12 FAM 262 Exhibit 262.3-1.

b. When contact reports, such as shown in 12 FAM 262 Exhibit 262.3-2, are filed by employees at post, RSOs or PSOs will review and evaluate the reported information and discuss the incident with the employee, providing counseling, as appropriate. Any facts or circumstances of a reported contact with individuals of any nationality must be promptly reported by the RSO or PSO to DS/ICI/CAS and the employee's parent agency if they appear to:

(1) Indicate an attempt, intention or reasonable potential to obtain unauthorized access to classified, sensitive, or proprietary information or technology; or

(2) Indicate the possibility of continued contact with the foreign national for such purposes.

12 FAM 262.3-2 Employee Responsibility

(TL:DS-62; 11-22-1999)
(Effective Date: 02-08-1999)

a. Employees and contractors should report immediately any contacts with individuals of any nationality under circumstances referred to in 12 FAM 262.1, paragraph a. In general, employee reporting should occur within one business day after such contact has occurred. If unable to report within this time frame, or unsure about the need to report at all, employees at post should notify the RSO or PSO as soon as practicable. If the RSO/PSO is unavailable, notify the administrative officer or the deputy chief of mission. Domestically, employees should promptly notify either DS/ICI/CAS or the security office of their parent agency, as appropriate.

b. Employees to whom these regulations apply shall use Form DS-1887, Contact Reporting Form, shown in 12 FAM 262 Exhibit 262.3-2, to report all contacts for which reports are required under paragraph a, above. If the official duty station is a U.S. mission abroad, the report must be submitted to either an RSO or PSO. If the official duty station is in the United States, employees and contractors of the Department of State shall send the contact report to DS/ICI/CAS.

c. As stated in 3 FAM 4100 - Employee Responsibility and Conduct, supervisors, rating officers, or other employees with firsthand knowledge of employee security concerns are obliged to bring them to the attention of appropriate post or agency officials.

12 FAM 262.3-3 Post Discretion

(TL:DS-45; 05-05-1995)

Posts may establish additional procedures to suit their particular security situations. Additional requirements should be discussed by the post counterintelligence working group (CIWG) and would be subject to approval by DS, in coordination with the security offices of parent agencies represented at posts abroad. All post requirements must be consistent with PDD/NSC-12.

12 FAM 262.3-4 Other Agency Discretion

(TL:DS-62; 11-22-1999)
(Effective Date: 02-08-1999)

As indicated in 12 FAM 262.1-1, paragraph b, agencies other than the Department of State which are under the authority of chiefs of mission abroad may also require their employees with special access clearances to follow additional reporting requirements, to the extent that such policies and requirements are consistent with PDD/NSC-12.

12 FAM 262.3-5 Contact Reports Originating at Post

(TL:DS-45; 05-05-1995)

The RSO or PSO will expedite employee contact reports to DS/ICI/CAS or through DS/ICI/CAS to the employee's parent agency. DS/ICI/CAS will also refer such information to the Central Intelligence Agency, following procedures agreed to between DS and the CIA.

12 FAM 262.3-6 Contact Reports Originating Domestically

(TL:DS-45; 05-05-1995)

DS/ICI/CAS will refer contact reports received domestically from employees or contractors of the Department of State to the Federal Bureau of Investigation, following procedures agreed to between DS and the FBI.

12 FAM 262.4 Accountability

(TL:DS-62; 11-22-1999)
(Effective Date: 02-08-1999)

Upon receiving a contact report and if DS/ICI/CAS perceives actual or potential security problems relating to an individual of any nationality, they will advise the employee to take appropriate precautions. Disciplinary action could result from an employee's failure to report a contact under the circumstances described in 12 FAM 262.1.

12 FAM 263 COUNTERINTELLIGENCE AWARENESS PROGRAM

12 FAM 263.1 Policy

(TL:DS-62; 11-22-1999)
(Effective Date: 02-08-1999)

a. The regional security officer (RSO) or the post security officer (PSO) will give an arrival briefing to all employees and contractors assigned to post on permanent change of station. The briefing will include information on counterintelligence. The RSO or PSO will make briefings available to adult dependents of employees and to contractors on a voluntary basis.

b. This policy applies to all executive branch agencies under the authority of a chief of mission.

c. For the purpose of this section, the term "contractor" is defined as a U.S. personal services contractor serving under the authority of a chief of mission or an employee of a commercial firm having a contract with the U.S. Government and serving under the authority of a chief of mission.

12 FAM 263.2 CI Awareness Training

(TL:DS-39; 08-15-1994)

The Counterintelligence and Special Investigations Division (DS/ICI/CAS) conducts counterintelligence (CI) and security awareness training programs, in coordination with the DS Training Center and other agencies, for the following employees:

- (1) Foreign Service officers;
- (2) Dependents of employees;
- (3) Ambassadors and deputy chiefs of mission;
- (4) Contractors and other Department personnel assigned to critical and high threat CI posts;
- (5) Regional security officers;
- (6) Diplomatic Security CI special agents;
- (7) Marine security guards;
- (8) Navy Seabees;
- (9) Diplomatic couriers;
- (10) U.S. military attachés; and
- (11) Other U.S. Government agency personnel, as required.

12 FAM 263.3 Post Procedures

(TL:DS-39; 08-15-1994)

Post threat levels are defined and identified in the Composite Threat List (classified) which is published by DS on a semi-annual basis.

12 FAM 263.3-1 Low, Medium, and High Counterintelligence Threat Posts

(TL:DS-62; 11-22-1999)

(Effective Date: 02-08-1999)

a. RSOs and PSOs will provide counterintelligence briefings to locally hired U.S. citizen employees under the authority of a chief of mission and ensure that Foreign Service nationals (FSNs) and third-country nationals (TCNs) are briefed in accordance with the FSN briefing program.

b. At high threat posts, RSOs and PSOs should provide counterintelligence briefings to temporary duty personnel and other official visitors. At low and medium threat posts, an unclassified written notice will be distributed to TDY personnel and other visitors giving them guidance on the local intelligence threat.

c. RSOs and PSOs will conduct departure security debriefings for all employees and contractors completing a tour of duty at a post *abroad*. The debriefing will include a discussion of counterintelligence matters. Should the RSO or PSO obtain information of a counterintelligence concern, he or she must forward a copy of the debriefing to DS/ICI/CAS which will forward a copy to the parent agency.

12 FAM 263.3-2 Critical Human Intelligence Threat Posts

(TL:DS-72; 01-26-2001)

(Effective Date: 02-08-1999)

a. In addition to the security awareness requirements cited in 12 FAM 264.3-1, the following additional instructions apply to posts that face a critical human intelligence (HUMINT) threat.

b. All executive branch agencies will review the proposed permanent assignment of all of their employees, contractors, and temporary duty personnel assigned in excess of 60 days accumulated in one year (not necessarily consecutive) to determine their suitability.

c. In the Department of State, the Investigations and Counterintelligence Division (DS/ICI/CI) reviews background investigations and personnel files on all Department employees proposed for permanent assignment to HUMINT threat posts. DS/ICI/CI evaluates security and suitability factors that could adversely affect suitability for assignment, in light of the heightened HUMINT threat, and any personal vulnerabilities potentially subject to HUMINT exploitation. DS/ICI/CI prepares a recommendation to the Director General of the Foreign Service with respect to an employee's suitability for assignment to a HUMINT threat post after considering the following circumstances:

(1) Whether the employee or an immediate family member has an immediate family member still residing in the proposed critical HUMINT threat country;

(2) Whether the employee or an immediate family member has other family ties in any critical HUMINT threat post where a foreign intelligence service (FIS) could exploit familial bonds of affection;

(3) Whether the employee has family member(s) currently or recently employed by the critical HUMINT threat country's military armed forces, intelligence or security service, police service, or ministry of foreign affairs;

(4) Whether the employee has a history of poor security practices (violations of 12 FAM 262 and 12 FAM 550) that are recent and of a serious nature;

(5) Whether the employee is or has been a known target of interest to a FIS;

(6) Whether the employee has a history of aberrant behavior such as drug or alcohol abuse or deviant sexual activities;

(7) Whether the employee has demonstrated emotional instability (as determined by MED);

(8) Whether the employee has exhibited financial or fiscal management irresponsibility;

(9) Whether a past investigation concerning the employee documents a serious allegation concerning misconduct, suitability, or professional ethics that could be exploited by a FIS;

(10) Whether the employee has had more than one previous assignment to the same critical HUMINT threat post;

(11) Whether the employee has made an unauthorized disclosure of sensitive or classified information;

(12) Whether the employee or close family member has demonstrated loyalty to the proposed critical HUMINT threat country of assignment (i.e., previously employed with the FIS or ministry of foreign affairs); and

(13) Whether the employee has had romantic involvement with citizen(s) of the proposed critical HUMINT threat country of assignment.

d. The Director General of the Foreign Service may accept or reject the recommendation made by DS for the proposed assignment to a critical HUMINT threat post. Upon request, DS will provide any pertinent information regarding the recommendation to the Director General.

e. The Personnel Security/Suitability Division (DS/ICI/PSS) reviews the background investigations of all contractors and employees of contractors proposed for assignment to critical HUMINT threat posts. DS uses the provisions of 12 FAM 263.3-2, paragraph b, 12 FAM 570, and 12 FAM 230 as a basis for adjudicating final determinations on suitability. When there are counterintelligence concerns, DS/ICI/PSS forwards the investigation to DS/ICI/CI. DS/ICI/CI reviews the investigation and offers a recommendation to DS/ICI/PSS. DS/ICI/PSS makes the final determination and forwards it to DS/ISP/INB to provide to the bureau requesting the contractor's assignment to a critical HUMINT threat post.

f. The RSO or PSO will provide CI briefings to locally hired U.S. citizen employees under the authority of a chief of mission, and ensure that FSNs and TCNs are briefed in accordance with the FSN briefing program.

g. The RSO or PSO will conduct a counterintelligence awareness refresher briefing with all employees annually. The RSO or PSO will make these refresher briefings available to adult dependents on a voluntary basis.

h. The RSO or PSO will conduct a routine departure security debriefing for all employees and contractors completing a tour of duty at a post abroad prior to the employee's or contractor's departure from post. The debriefing will include a discussion of counterintelligence matters. Should the RSO or PSO obtain information of a counterintelligence concern, he or she must forward a copy of the debriefing to DS/ICI/CAS, which will forward a copy to the parent agency.

i. The RSO will notify DS/ICI/CAS and the RSO at a gaining post of personnel transfers so that debriefings can be scheduled. All employees completing a tour of duty must receive a special in-depth counterintelligence debriefing conducted by DS/ICI/CAS or, in the case of direct transfers, by the RSO or PSO of the gaining post. All contract personnel must receive a special counterintelligence debriefing by either DS/ICI/CAS or the contractor. All temporary duty (TDY) employees must receive a special counterintelligence debriefing upon completion of the temporary duty conducted by DS/ICI/CAS or, in the case of TDY from one post to another, by the RSO or PSO of the post of residence. Employees or contract personnel of agencies other than State who are returning to Washington, D.C., shall be debriefed by the security office of their parent agency; when transferring between posts, the RSO or PSO at the gaining post shall debrief other agency personnel to report security concerns or information of interest to their agency or to future travelers. Copies of all special debriefings should be sent to DS/ICI/CAS by the RSO/PSO, which will forward a copy to parent agencies. PSOs must also send a copy to the RSO. The RSO will notify DS/ICI/CAS and the RSO at a gaining post of personnel transfers so that debriefings can be scheduled.

12 FAM 263.4 Domestic Programs

(TL:DS-62; 11-22-1999)

(Effective Date: 02-08-1999)

a. State only: The Analysis and Special Projects Branch (DS/CAS/ASP) provides individual and post-specific domestic counterintelligence training on a formal and ad hoc basis.

b. In cooperation with DS/ICI/CAS, the Foreign Service Institute (M/FSI) sponsors programs for employees assigned to selected critical threat posts. New Department employees attending FSI orientation also receive a segment on counterintelligence awareness.

c. DS/CAS/ASP tailors specific programs for specialty professions such as cleared U.S. citizen guards, communicators, Seabees, etc.

d. State only: DS/CAS/ASP arranges for or provides post-specific briefings for individuals on a need-to-know basis.

e. DS/CAS/ASP also provides CI briefings and policy support to other USG agencies.

12 FAM 264 PERSONAL TRAVEL TO CRITICAL HUMAN INTELLIGENCE THREAT COUNTRIES

12 FAM 264.1 Scope and Applicability

12 FAM 264.1-1 Scope

(TL:DS-42; 11-30-1994)

a. These standards, which were cleared by the Overseas Security Policy Group (OSPG), apply to all agencies under the authority of a chief of mission (COM).

b. The requirements govern travel to countries with a critical human intelligence threat post identified in the DS/ICI/CAS semi-annual composite threat list and to certain countries with which the United States does not have diplomatic relations. Employees should consult with DS/ICI/CAS for specific countries where these posts are located.

12 FAM 264.1-2 Program Responsibility

(TL:DS-42; 11-30-1994)

The Office of Counterintelligence Programs (DS/ICI/CAS) directly administers this program for Department employees stationed domestically, and indirectly through the regional security officer (RSO) or post security officer (PSO) at Foreign Service posts.

12 FAM 264.2 Procedures

(TL:DS-72; 01-26-2001)

(Effective Date: 02-08-1999)

a. The criteria in the paragraphs that follow in this section apply to travel to countries in which critical human intelligence threat posts are located, regardless of the threat level where the employee is stationed or departs from.

b. All U.S. Government employees under the authority of a chief of mission must notify the RSO or PSO at post of residence in advance of intended personal travel to any country with a critical human intelligence threat post, including travel with tour groups. Employees stationed domestically directly notify DS/ICI/CAS. Provide this information at least three weeks before starting travel.

c. Each employee must provide a notification of personal travel by using the item format contained in 12 FAM 264 Exhibit 264.2. The RSO, PSO, or DS/ICI/CAS will retain this information as part of the permanent record.

d. The RSO, PSO, or DS/ICI/CAS will provide pertinent information from the travel notification to U.S. embassies in the countries listed on the itinerary at least two weeks prior to the traveller's intended departure. (Use the format given in 12 FAM 264 Exhibit 264.2.) RSOs and PSOs will also provide copies of their communications to DS/ICI/CAS and to the security office of the traveller's parent agency.

e. The RSO, PSO, or DS/ICI/CAS, as appropriate, will ensure that each traveller receives a defensive security briefing prior to their travel.

f. Travellers must immediately contact the nearest U.S. consul, attaché, RSO, or duty officer if detained or subjected to significant harassment or provocation while travelling. Upon return to post of residence or the Department, the traveller should report any unusual incidents, including those of potential security concerns, to the RSO, PSO, or DS/ICI/CAS, as appropriate. RSOs and PSOs will in turn report unusual incidents, detention, harassment, provocation, etc. to DS/ICI/CAS, which forwards copies of the reports to the traveller's parent agency.

g. Employees having access to sensitive compartmented information (SCI) have a special security obligation and are required to give advance notification to the SCI control officer at their duty station of their plans to travel to a country with a critical human intelligence threat post, or any country so designated by the Attorney General. Prior to such travel, persons with SCI clearances must receive a defensive security briefing from their SCI control officer. These special restrictions apply while actively holding SCI clearances and for one year after access to SCI has been terminated.

h. The Department encourages spouses and adult dependents of employees to advise the RSO, PSO, or DS/ICI/CAS as appropriate of their personal travel, and to receive any available defensive security briefings, especially those at post of residence.

12 FAM 265 THROUGH 269 UNASSIGNED

12 FAM 262 Exhibit 262.3-1
ACKNOWLEDGEMENT OF POLICY
GOVERNING OFFICIAL AND PERSONAL
RELATIONSHIPS WITH FOREIGN
NATIONALS FROM DESIGNATED
COUNTRIES, AND CONTACT REPORTING
RESPONSIBILITIES (FORMAT)

(TL:DS-62; 11-22-1999)
(Effective Date: 02-08-1999)

This is to acknowledge that:

I have been briefed on this policy and understand my responsibilities to report contacts and associations with individuals from designated countries;

I understand that this policy applies to all U.S. Government employees on official duty abroad who are under the authority of the chief of mission;

I understand that my failure to comply with this policy provides grounds for appropriate disciplinary action;

I understand that I should caution my adult dependents about the potential threat from foreign intelligence services and encourage them to report any attempts by foreign nationals to exploit them;

I understand that if I have any questions regarding this policy, I should raise them with the regional security officer or post security officer while abroad and the Department of State's Bureau of Diplomatic Security (DS/ICI/CAS) when in the United States.

Signature

Signature Date

Employee Name (typed or printed)

Witnessing Official's
Name and Title

Position

Post

Agency

12 FAM 262 Exhibit 262.3-2 FORM DS-1887 CONTACT REPORTING FORM

(TL:DS-72; 01-26-2001)



U. S. Department of State

SECRET/NOFORN
When Completed

CONTRACT REPORTING

PRINT OR TYPE ALL INFORMATION EXCEPT FOR SIGNATURE

RSO/PSO or other recipient		Post and Section or Office Symbols
Reporting Employee Name		Agency
Signature	Date (mm-dd-yyyy)	Post and Section or Office Symbols
<p>Before you complete this report, please reflect on each of the following, which MAY be indicative of an intelligence approach. Did your contact:</p> <ol style="list-style-type: none"> 1. Actively seek a close personal association or unsolicited recurring contacts? Give gifts? 2. Interject a third party into the relationship? 3. Repeatedly appear in "chance encounters," including those at large social gatherings? 4. Provide or seek political, economic, military, or sensitive information outside of official channels? 5. Solicit biographical information or gossip about other mission personnel? Disclose such information about himself or herself, or others? 6. Suggest or encourage illegal activity, such as black marketing, unauthorized currency exchanges, etc.? <p>When answering, use "None" where applicable. Do not use "N/A" or "Not Applicable."</p>		
Contact's Name		Nationality
Title/Position		Type of Relationship (check one) <input type="checkbox"/> Official <input type="checkbox"/> _____
Provide as much biographical data on the contact as possible		

DECL: OADR

DS-1887
07-2000

12 FAM 264 Exhibit 264.2
NOTIFICATION OF PERSONAL TRAVEL TO
CRITICAL HUMAN INTELLIGENCE THREAT
POST/COUNTRY
(FORMAT)

(TL:DS-72; 01-26-2001)

Use either a telegram or memorandum as appropriate.

SECRET/NOFORN
(When Completed)

DATE:

TO: (RSO; PSO; DS/ICI/CAS)

FROM: (Name/Agency) (Post/Section)

TAGS/TERMS: ASEC (and others as appropriate, such as country TAGS)

SUBJECT: Personal Travel to Critical Human Intelligence Threat Post
Country(ies)

In accordance with 12 FAM 265.2, you are hereby advised of the intended travel to a country with a critical human intelligence threat post. Missions in countries to be visited will respond to this notification only if there is objection to the trip or any aspect thereof.

1. Name of Traveller:
2. Date/Location of Birth:
3. Passport Number and Type:
4. Employing Department or Agency:
5. Title/Functional Position:
6. Names of accompanying dependents (date(s)/place(s) of birth, passport number(s)):
7. Purpose, itinerary, dates, and means of travel:
8. Address in each country on itinerary:
9. Tour, group, or travelling companions:

Continuation - 12 FAM 264 Exhibit 264.2

10. If traveller or companion has relatives or friends in countries on itinerary, give name, relationship, address, and phone number (if known) and indicate whether contact is to be made:
11. If, under the laws of the country(ies) to be visited, the traveller has been or might still be a citizen of that country, please give details:

You may also give additional details as appropriate.

SECRET/NOFORN

(When Completed)

DECLASSIFY: OADR